(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
22 February 2001 (22.02.2001)

PCT

(10) International Publication Number
WO 01/13201 A3

(51) International Patent Classification[7]: H04L 29/06, G06F 1/00

(21) International Application Number: PCT/US00/21965

(22) International Filing Date: 11 August 2000 (11.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/148,624 12 August 1999 (12.08.1999) US
Not furnished 4 August 2000 (04.08.2000) US

(71) Applicant: SARNOFF CORPORATION [US/US]; 201 Washington Road, CN-5300, Princeton, NJ 08543 (US).

(72) Inventor: WALDMAN, Harvey; 947 Pickering Drive, Yardley, PA 19067 (US).

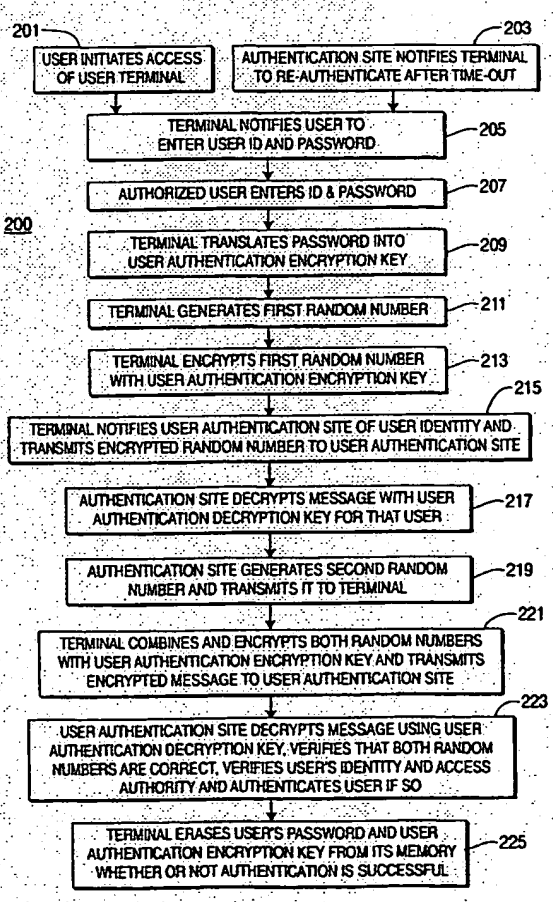
(74) Agent: PATTERSON, William, B.; Thomason, Moser & Patterson, L.L.P., Suite 1500, 3040 Post Oak Boulevard, Houston, TX 77056 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE,

[Continued on next page]

(54) Title: PEER-TO-PEER NETWORK USER AUTHENTICATION PROTOCOL



(57) Abstract: In a peer-to-peer network having a plurality of user terminals, each capable of serving as a user authentication site for other terminals of the network and having an open side of a firewall and a secure side of the firewall, a method for authenticating a user. A user authentication database is stored in memories in the secure side of first and second terminals of the network. The first terminal receives a password from the user, and translates the password into an authentication encryption key for the user. The first terminal generates a first random number, encrypts the first random number with the authentication encryption key to provide a first encrypted message, and transmits the first encrypted message to the second terminal, which serves as a user authentication site for the first terminal. The user authentication site decrypts the encrypted first message to provide the first random number, and generates a second random number, which is transmitted to the first terminal. The first terminal combines and encrypts the first and second random numbers, with the authentication encryption key, to provide a second encrypted message. The first terminal transmits the second encrypted message to the user authentication site, which decrypts the encrypted second message to provide the combined first and second random numbers. The user authentication site verifies that the first and second random numbers are correct, and authenticates the user in accordance with this verification.

WO 01/13201 A3

IT, LU, MC, NL, PT, SE). OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
6 December 2001

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Inter ional Application No
PCT/US 00/21965

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, COMPENDEX, IBM-TDB

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	KWON T ET AL: "Authenticated key exchange protocols resistant to password guessing attacks" IEE PROCEEDINGS: COMMUNICATIONS, INSTITUTION OF ELECTRICAL ENGINEERS, GB, vol. 145, no. 5, 13 October 1998 (1998-10-13), pages 304-308, XP006010921 ISSN: 1350-2425	1,2,5,9
Y	page 305, left-hand column, paragraph 3.1 -page 307, left-hand column, paragraph 36	7,8
A	---	3,4
Y	WO 95 24698 A (BULL CP8) 14 September 1995 (1995-09-14)	7,8
A	page 5, line 11 - line 15 page 6, line 16 -page 7, line 14	6
A	page 24, line 17 -page 26, line 8	3,4
	--- -/--	

[X] Further documents are listed in the continuation of box C. [X] Patent family members are listed in annex.

° Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
16 August 2001	23/08/2001

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Karavassilis, N

Inter 'ional Application No
PCT/US 00/21965

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 406 628 A (BELLER MICHAEL J ET AL) 11 April 1995 (1995-04-11) column 14, line 30 - line 56	1

INTERNATIONAL SEARCH REPORT

Information on patent family members

Intr ional Application No
PCT/US 00/21965

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9524698 A	14-09-1995	US 5293424 A	08-03-1994
		EP 0596276 A	11-05-1994
		FI 955307 A	06-11-1995
		KR 232086 B	01-12-1999
		NO 954438 A	05-01-1996
		AT 180587 T	15-06-1999
		DE 69325072 D	01-07-1999
		DE 69325072 T	28-10-1999
		DK 596276 T	21-02-2000
		ES 2135432 T	01-11-1999
		JP 6208515 A	26-07-1994
		SG 48001 A	17-04-1998
US 5406628 A	11-04-1995	US 5299263 A	29-03-1994
		CA 2157011 A,C	15-09-1994
		DE 69426416 D	18-01-2001
		DE 69426416 T	26-07-2001
		EP 0691055 A	10-01-1996
		JP 8507619 T	13-08-1996
		WO 9421067 A	15-09-1994